Kush po sulmon rrjetin tonë?
Kërcënimi, Vulnerabiliteti dhe Rreziku

- Kërcënimet
  - Rreziku potencial për një aset të tillë siq janë të dhënat ose rrjeti.
  - Vulnerabiliteti dhe Sipërfaqja e Sulmit
  - Dobësia në një sistem që mund të shfrytëzohet nga një kërcënim.
  - Sipërfaqja e sulmeve përshkruan pika të ndryshme ku një sulmues mund të futet në një sistem dhe mund të marrë të dhënat (Shembull - sistemi operativ pa patch sigurie)
- Shfrytëzimi
  - Ky mekanizmëm përdoret për të nxitur një dobësi apo për të kompromet uar një pasuri.
  - Remote - punon mbi rrjetin.
  - Kërcënuesi lokal ka qasje përdoruesi ose administrativ në sistemin e fundit.
- Rreziku
  - Ndjeshmëria që një kërcënim do të shfrytëzojë një cenueshmëri të një aseti dhe do të rezultojë në një pasojë të padëshirueshme.

Kush po sulmon rrjetin tonë?
Hackers vs Threat

- White Hat Hackers
  - Hakerat etikë që përdorin aftësitë e tyre të programimit për qëllime të mira, etike dhe ligjore.
  - Kryejnë teste penetrimi për të zbuluar dobësitë dhe I raportojnë tek zhvilluesit para shfrytëzimit.
- Grey Hackers Hat`
  - Kryejnë krime dhe bëjnë gjëra jo etike, por jo për përfitime personale ose për të shkaktuar dëme.
  - Mund të kompromet ojë rrjetin dhe më pas të zbulojnë problemin në mënyrë që organizata të mund të rregullojë problemin.
- Hackers Black Hat
  - Kriminelët joetikë që shkelin sigurinë për përfitime personale, ose për arsye të dëmshme, siç janë rrjetet sulmuese.
- **Shënim: Akterët e kërcënimeve janë term që përdoret për të përshkruar hakerat e hirit gri dhe të zeza.**

Kush po sulmon rrjetin tonë?
Evolucioni i akterëve të kërcënimit

- Script Kiddies
- Hakerat e papërvojë që drejtojnë mjete ekzistuese dhe shfrytëzon ato, për të shkaktuar dëm, por zakonisht jo për fitim.
- Kapele të bardha apo të zeza që vjedhin sekretet qeveritare, mbledhin informata inteligjente dhe rrëzojnë rrjetet.
  - Synimet janë qeveritë e huaja, grupet terroriste dhe korporatat.
- Kriminelët kibernetikë
  - Kapele të zeza vjedhin miliarda dollarë nga konsumatorët dhe bizneset.
- Hacktivists
  - Kapele gri që protestojnë kundër ideve politike dhe shoqërore.
  - Shkruajnë artikuj dhe video për të zbuluar informacione të ndjeshme.

Kush po sulmon rrjetin tonë?
Kriminelët kibernetikë

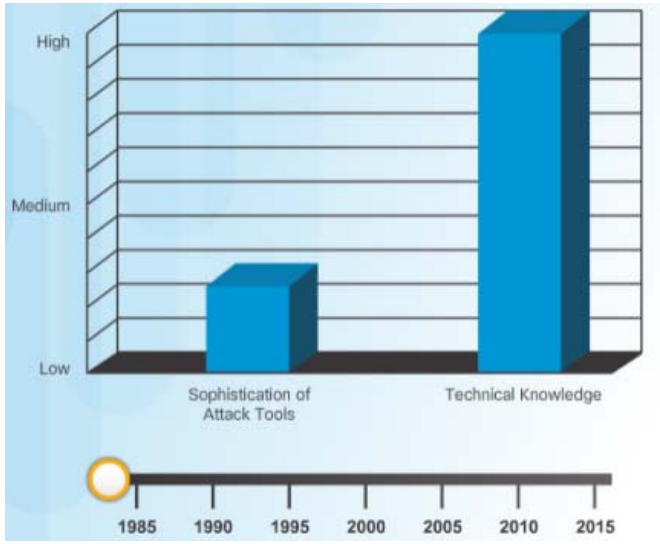
- Akterët e kërcënimit të motivuar nga paratë.
- Blejnë, shesin dhe tregtojnë informacionin privat dhe pronën intelektuale.
- Vjedhin nga konsumatorët, bizneset e vogla, si dhe ndërmarrjet dhe industritë e mëdha.

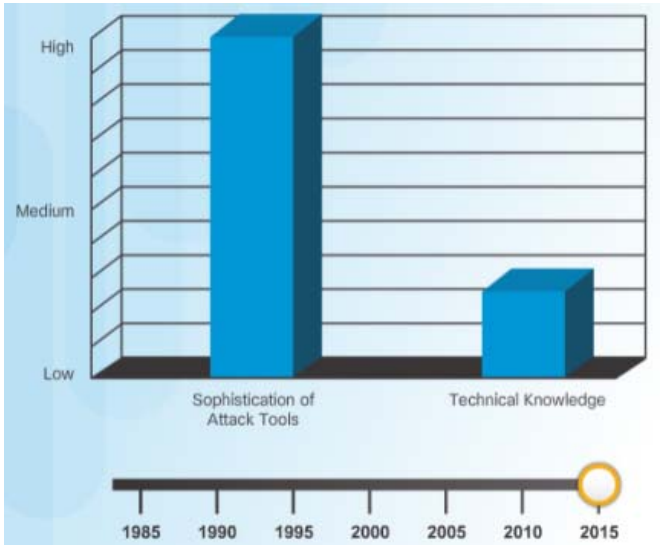
Kush po sulmon rrjetin tonë?
Detyrat e Cybersecurity

- Zhvillojnë vetëdije të mirë të sigurisë kibernetike
- Raporton krimin kibernetik ndaj autoriteteve.
- Janë të vetëdijshëm për kërcënimet e mundshme në email dhe në internet
- Ruajnë informacione të rëndësishme nga vjedhja.
- Organizatat duhet të ndërmarrin veprime dhe të mbrojnë asetet, përdoruesit dhe klientët e tyre.

Mjetet e Aksionit të Kërcënimit
Prezantimi i mjeteve sulmuese

- Sulmuesit përdorin mjete për të shfrytëzuar një dobësi.
- Sofistikimi i mjeteve të sulmeve dhe njohurive teknike për të kryer sulme ka ndryshuar që nga viti 1985.





Mjetet e Aksionit të Kërcënimit
Kategoritë e sulmeve

- Kategoritë e përbashkëta të sulmeve në rrjet
  - Përgjimi - kapni dhe dëgjoni trafikun e rrjetit.
  - Modifikimi i të dhënave - ndryshon të dhënat e kapura në pako pa dijeninë e dërguesit ose marrësit.
  - IP spoofing adresa - ndërton një paketë IP që duket se ka origjinën nga një adresë e vlefshme brenda intranetit të korporatës.
  - Fjalëkalimi i bazuar - përdor llogaritë e vjedhura për të marrë listat e përdoruesve të tjerë dhe informacionin e rrjetit.
  - Mohimi i Shërbimit - parandalon përdorimin normal të një kompjuteri ose rrjeti nga përdoruesit e vlefshëm.
  - Man-in-the-Middle Attack - hakerat e vendosin veten midis një burimi dhe destinacioni për të monitoruar, kapur dhe kontrolluar komunikimin.
  - Compromised-Key - të fitojë qasje në një komunikim të siguruar pa dërguesin ose marrësin duke qenë në dijeni të sulmit duke marrë çelësin e fshehtë.

malware
Llojet e Malware

- Malware
  - I shkurtër për softuer me qëllim të keq ose kod me qëllim të keq.
  - Projektuar në mënyrë specifike për të dëmtuar, prishur, vjedhur ose shkaktuar veprime të paligjshme në hostet ose rrjetet e të dhënave.

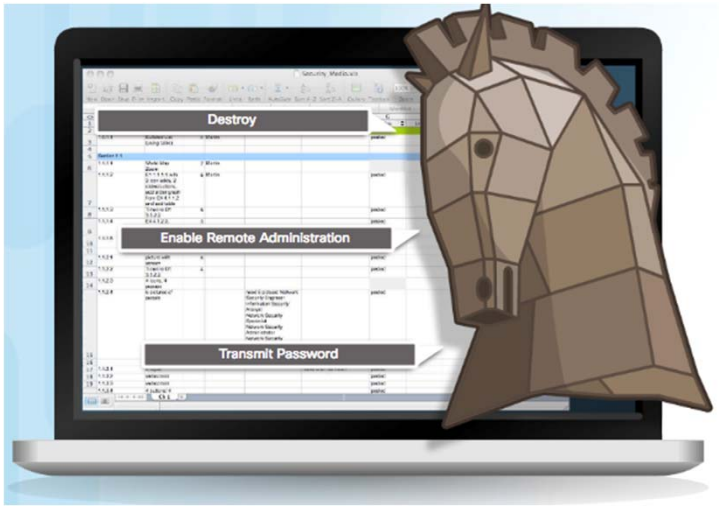
malware
Viruset

- Lloji i malware që propagandon duke futur një kopje të vetes në një program tjetër.
- Përhapen nga një kompjuter në tjetrin, duke infektuar kompjuterë.
- Përhapet nga disqet e kujtesës USB, CD, DVD, aksione të rrjetit dhe email.
- Mund të rrij I qetë dhe të aktivizohet në një kohë dhe datë specifike.
- Kërkon veprime njerëzore për të futur kodin keqdashës në një program tjetër.
- Ekzekuton një funksion të veçantë të padëshiruar dhe shpesh të dëmshëm në një kompjuter.

malware
Trojan Horses

- Kodi keqdashës që është dizajnuar të duket legjitim.
- Shpesh gjendet I bashkangjitur tek lojërat online.
- Shfrytëzon privilegjet e përdoruesit që drejton malware.
- Mund të shkaktojë dëme të menjëhershme, të sigurojë qasje nga largët në sistem ose të futet përmes një derë të pasme (backdoor).

malware
Klasifikimi i Trojan Horse

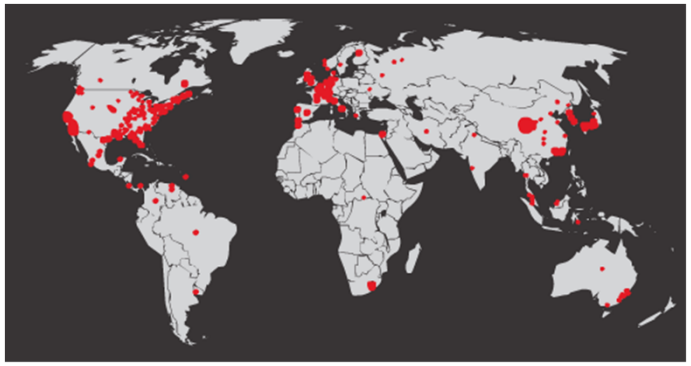


- **Kali i Trojës me qasje të largët - Mundëson qasje të largët të paautorizuar.**
- **Kalimi i të dhënave duke dërguar Kali i Trojës - Siguron akterin e kërcënimit me të dhëna të ndjeshme, të tilla si fjalëkalime.**
- **Kali i Trojës shkatërrues - Korrupton ose fshin skedarët.**
- **Proxy trojan - Do të përdorë kompjuterin e viktimës si mjet burimor për të nisur sulme dhe për të kryer aktivitete të tjera të paligjshme.**
- **FTP Kali i Trojës - Mundëson shërbime të transferimit të paautorizuar të skedarëve në pajisjet e paautorizuara.**
- **Softueri i sigurisë çaktivizues Kali trojan - Ndalon programet antivirus ose firewalls nga funksionimi.**
- **DoS trojan kali - Ngadalëson ose ndalon aktivitetin e rrjetit.**

malware
Worms

- Ekzekuton kodin arbitrar dhe instalon veten në kujtesën e pajisjes së infektuar.
- Automatikisht përsëritet dhe përhapet në të gjithë rrjetin nga sistemi në sistem.
- Komponentët e një sulmi të krimbave përfshijnë një dobësi të shfrytëzuar, duke ofruar një ngarkesë me qëllim të keq dhe vetëpërhapje.
- Virus kërkon një program pritës për tu aktivizuara ndërsa Worm mund të funksionojë vetë.

Initial Code Red Worm Infection – 658 servers

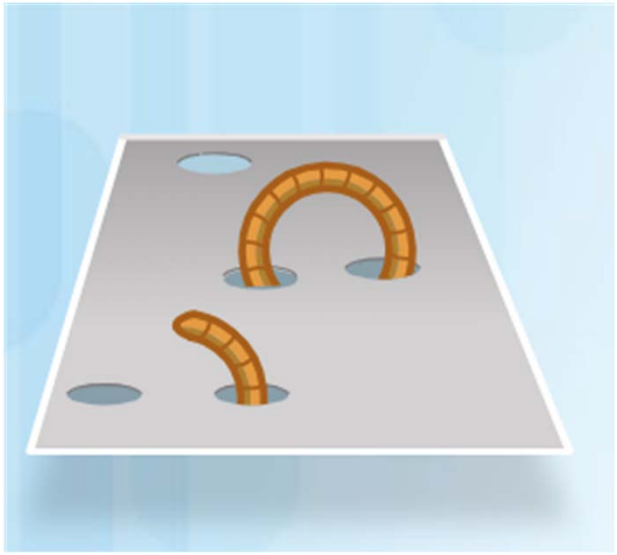


Code Red Worm Infection– 19 Hours Later
300,000 servers

Malware

Komponentet e Worms

- Sulmet e rrafshët (Flat Attacks) përbëhen nga tre komponentë:
  - Aktivizimi i cenueshmërisë - Worm instalon veten duke përdorur një mekanizëm shfrytëzimi, si një shtojcë e-mail, një skedë ekzekutuese ose një kalë trojan, në një sistem të prekshëm.
  - Mekanizmi i propagimit - Pasi të ketë qasje në një pajisje, krimbi përsëritet dhe vendos objektiva të reja.
  - Shitës me pagesë - Çdo kod me qëllim të keq që rezulton në ndonjë veprim është një ngarkesë e cila përdoret për të krijuar një backdoor që lejon një qasje të kërcënimit në hostin e infektuar ose për të krijuar një sulm DoS.



malware
ransomware

- Malware që mohon qasjen në sistemin kompjuterik të infektuar ose të dhënat e tij.
- Kriminelët kibernetikë kërkojnë pagesë për lirimin e sistemit kompjuterik.
- Shpesh përdor një algoritëm të enkriptimit për të koduar skedarët dhe të dhënat e sistemit, nuk mund të decrdekriptohet lehtë.
- Email-i dhe reklamat me qëllim të keq janë vektorë për fushatat ransomware.
- Inxhinieria sociale përdoret gjithashtu, kriminelët kibernetikë që identifikohen si teknikë të sigurisë telefonojnë shtëpitë dhe bindin përdoruesit që të lidhen me një faqe interneti që shkarkon ransomware në kompjuterin e përdoruesit.

malware
Malware të tjera

- Malwaret Modern
  - Spyware - Përdoret për të mbledhur informacion rreth një përdoruesi dhe për të dërguar informacionin në një entitet tjetër pa pëlqimin e përdoruesit. Mund të jetë një monitor i sistemit, Adware, Cookies, dhe Key Loggers.
  - Adware - Në mënyrë tipike shfaq pop-ups për të gjeneruar të ardhura për autorin e saj. Mund të analizojë interesat e përdoruesit duke ndjekur faqet e vizituara dhe dërgimin e reklamave pop-up në ato vende.
  - Scareware - Përfshin softuerin e mashtrimit që përdor inxhinieri sociale për të bindur ose nxitur për të krijuar perceptimin e një kërcënimi. Drejtuar në përgjithësi në një përdorues që nuk dyshon dhe përpiqet të bindë përdoruesin të infektojë një kompjuter duke ndërmarrë veprime për të adresuar kërcënimin fals.
  - Phishing - Përpjekjet për t'i bindur njerëzit që të zbulojnë informacione të ndjeshme. Shembujt përfshijnë marrjen e një email nga banka e tyre duke i kërkuar përdoruesve të zbulojnë llogarinë e tyre dhe numrat PIN.
  - Rootkits – Instalohet në një sistem të kompromet uar. Pasi ajo është instaluar, ajo vazhdon të fshehë ndërhyrjen e saj dhe të sigurojë qasje të privilegjuar.

Sjelljet e Zakonshme të Malware

- Kompjuterët e infektuar me malware shpesh shfaqin një ose më shumë efekte nga këto:
  - Shfaqja e skedarëve, programeve ose ikonave të çuditshme në desktop.
  - Programet antivirus dhe firewall fiken ose rikonfigurojnë atributet.
  - Ekrani i kompjuterit është bllokohet ose sistemi crash.
  - Email-et dërgohen në mënyrë spontane pa dijeninë tuaj në listën tuaj të kontakteve.
  - Skedarët janë modifikuar ose fshirë.
  - Rritet shfrytëzimi I resurseve të CPU si dhe pëërdorimi i RAM memories.
  - Shfaqen problem të ndërlidhura me rrjetin kompjuterik.
  - Ngadalësohet shpejtësia e kompjuterit ose shfletuesit të uebit.
  - Aktivizohen procese dhe shërbime të panjohura.
  - Hapen porte të pashfrytëzuara TCP ose UDP.

Sulmet e Rrjetit të Përbashkët
Llojet e sulmeve në rrjet

- Ne klasifikojmë sulmet në tri kategori kryesore:

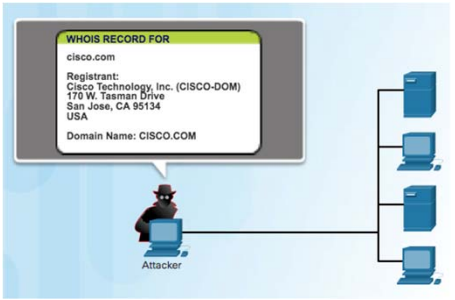
- Duke kategorizuar sulmet e rrjetit, është e mundur të trajtohen llojet e sulmeve dhe jo sulmet individuale.

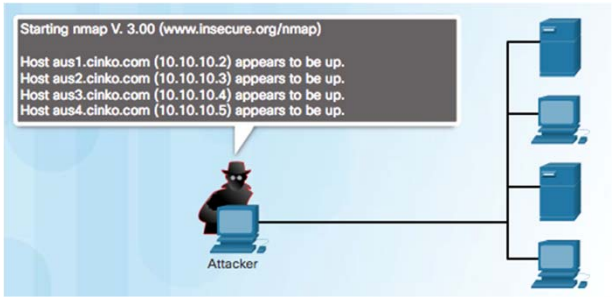
Sulmet e Rrjetit të Përbashkët
Sulmet e zbulimit

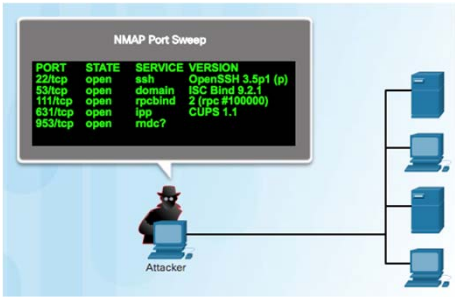
- Njohur gjithashtu si mbledhje informacioni, sulmet zbuluese kryejnë zbulimin e paautorizuar dhe hartën e sistemeve, shërbimeve ose dobësive.
- Shembull analog: Një hajdut që vëzhgon një lagje duke shkuar derë më derë duke pretenduar se ka për tshitur diçka.
- Sulmet e Recon paraprijnë sulmet ndërhyrëse të hyrjes ose sulmet ndaj DoS dhe përdorin përdorimin e mjeteve gjerësisht të disponueshme.

Sulmet e Rrjetit të Përbashkët
Shembuj të sulmeve zbuluese

- Teknikat e përdorura nga Sulmuesit:
  - Nisja e një skanimi të porteve të adresave IP aktive - Sulmuesi inicion skanimet e porteve në hostët e identifikuar nga ping për të përcaktuar se cilat porte ose shërbime janë në dispozicion.
  - Mjetet e skanimit të portit si Nmap, SuperScan, dhe Veglat NetScan iniciojnë lidhjet me hostët e synuar duke skanuar për portet që janë të hapura në kompjuterët e synuar.







Sulmet e Rrjetit të Përbashkët
Qasja e sulmeve

- Qasja e sulmeve shfrytëzon dobësitë në shërbimet e caktuara p.sh shërbimet FTP dhe shërbimet e uebit për të marrë të dhëna, për të fituar qasje në sisteme ose për të përshkallëzuar privilegjet e qasjes.

- Ka të paktën tre arsye që sulmuesit do të përdorin sulme në qasje apo në rrjete ose sisteme:
  - Për të rifituar të dhënat
  - Për të fituar qasje në sistemet
  - Për të përshkallëzuar privilegjet e qasjes

Sulmet e Rrjetit të Përbashkët
Llojet e sulmeve të qasjes

- **Sulmi me fjalëkalim - Përpjekje për të zbuluar fjalëkalime të sistemit kritik duke përdorur sulme phishing, sulme me fjalor, sulme brutale, ose duke përdorur teknika të inxhinierisë sociale.**
- **Pass-the-hash - Ka qasje në kompjuterin e përdoruesit dhe përdor malware për të fituar qasje në hash fjalëkalimin e ruajtur. Sulmuesi pastaj përdor hash për të authentikuar në serverë të tjerë të largët ose pajisje.**
- **Shfrytëzimi i besueshmërisë - Përdorin një qasje të besuar për të fituar qasje në burimet e rrjetit.**
- **Redirection port - Përdor një sistem të kompromet uar si një bazë për sulme kundër objektivave të tjera.**
- **Sulmi Man-in-the-Middle - Sulmuesi është i pozicionuar në mes të dy njësive legjitime për të lexuar, modifikuar ose përcjellë të dhënat që kalojnë mes dy palëve.**
- **IP, MAC, DHCP Spoofing - Një pajisje përpiqet të paraqesë si një tjetër duke falsifikuar të dhënat e adresës.**

Sulmet e Rrjetit të Përbashkët
Sulmet e Inxhinierisë Sociale

- Lloji i qasjes që tenton të manipulojë individët në kryerjen e veprimeve ose zbulimin e informacionit konfidencial të nevojshëm për të hyrë në një rrjet.
  - Shembuj të sulmeve inxhinierike sociale përfshijnë:
    - Pretekst - Thirrje individuale dhe gënjeshtra ndaj tyre në një përpjekje për të fituar qasje në të dhëna të privilegjuara. Pretendon të ketë nevojë për të dhëna personale ose financiare në mënyrë që të konfirmojë identitetin e marrësit.
    - Spam - Përdorin email spam për të mashtruar një përdorues duke klikuar një lidhje të infektuar ose duke shkarkuar një skedar të infektuar.
    - Phishing - versioni i Përbashkët është sulmuesi që i dërgon individëve me entuziazëm një porosi me qëllim identifikimi, me shpresë që përdoruesi i synuar të klikojë në një lidhje ose të shkarkojë kodin e dëmshëm.
    - Diçka për Diçka (Quid pro quo) - Kërkon informacion personal nga një palë në këmbim të diçkaje si një dhuratë falas.
    - Tailgating - Ndjek një person të autorizuar me një simbol të korporatës në një vend të sigurt.
    - Baiting - Sulmuesi lë një pajisje fizike të infektuar me malware, të tilla si një flash drive USB në një vend publik, si një banjë e korporatave. Ai që e gjen pajisjen dhe fut atë në kompjuterin e tyre.
    - Hacking vizuale - Fizikisht vëzhgon viktimën duke u qasur përmes kredencialeve personale si një login në workstation, një PIN ATM, ose kombinim në një lock fizike. Gjithashtu i njohur si "surfing sup".

Sulmet e Rrjetit të Përbashkët
Sulmet ndaj rrjetëzimit social

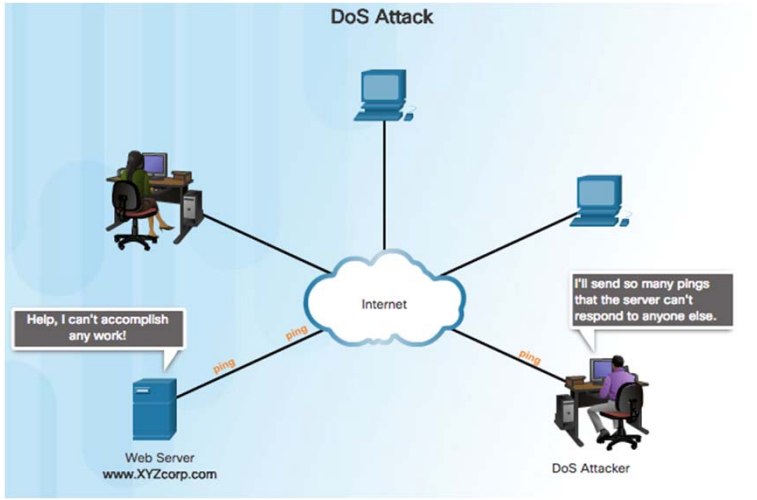
- Phishing
  - Teknika e zakonshme e inxhinierisë social që kërcënojnë sulmuesit të dërgojnë email që duket se janë nga një organizatë legjitime (si një bankë)
  - Ndryshimet përfshijnë:
    - Phishing - Sulmi phishing i synuar dhe i përshtatur për një individ ose organizatë specifike dhe ka më shumë gjasa të mashtrojë me sukses objektivin.
    - Whaling Attack - Ngjashëm me phishing, por është e përqendruar në objektiva të mëdha të tilla si drejtuesit e lartë të një organizate.
    - Pharming - Komprometon shërbimet e emrit të domenit duke injektuar shënimet në skedarët lokal. Pharming gjithashtu përfshin helmimin e DNS duke kompromentuar serverat DHCP që specifikojnë serverat DNS te klientët e tyre.
    - Watering holle attack- Përcakton faqet e internetit që një grup i synuar viziton rregullisht dhe përpiqet të kompromet ojë ato faqe interneti duke i infektuar ata me malware që mund të identifikojnë dhe targetojnë vetëm anëtarët e grupit të synuar.
    - Vishing attack - Sulmi Phishing duke përdorur zërin dhe sistemin e telefonit në vend të email-it.
    - Smishing Attack - Sulmi Phishing duke përdorur SMS texting në vend të email.

Sulmet e Rrjetit të Përbashkët
Forcimi i lidhjes më të dobët

- Njerëzit janë zakonisht lidhja më e dobët në sigurinë kibernetike
- Organizatat duhet të trajnojnë në mënyrë aktive personelin e tyre dhe të krijojnë një "kulturë të vetëdijshme për sigurinë".

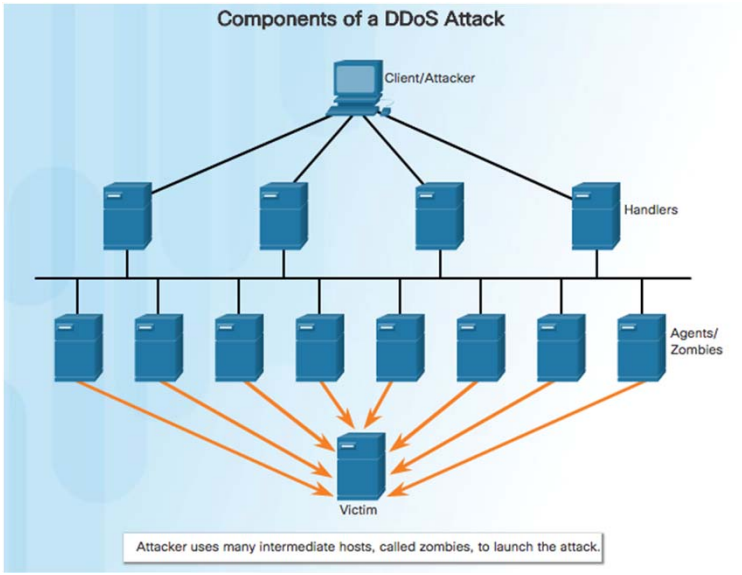
Sulmet e Rrjetit të Përbashkët
Sulmet e Mohimit të shërbimit

- Në mënyrë tipike rezultojnë në një lloj ndërprerje të shërbimit ndaj përdoruesve, pajisjeve ose aplikacioneve.
- Mund të shkaktohet nga mbizotërimi i një pajisjeje të synuar me një sasi të madhe trafiku ose duke përdorur paketa me format të dëmtuar me qëllim të keq.
- Një sulmues përcjell paketat që përmbajnë gabime që nuk mund të identifikohen nga aplikacioni, ose dërgon pako të formatuara në mënyrë të pasaktë.

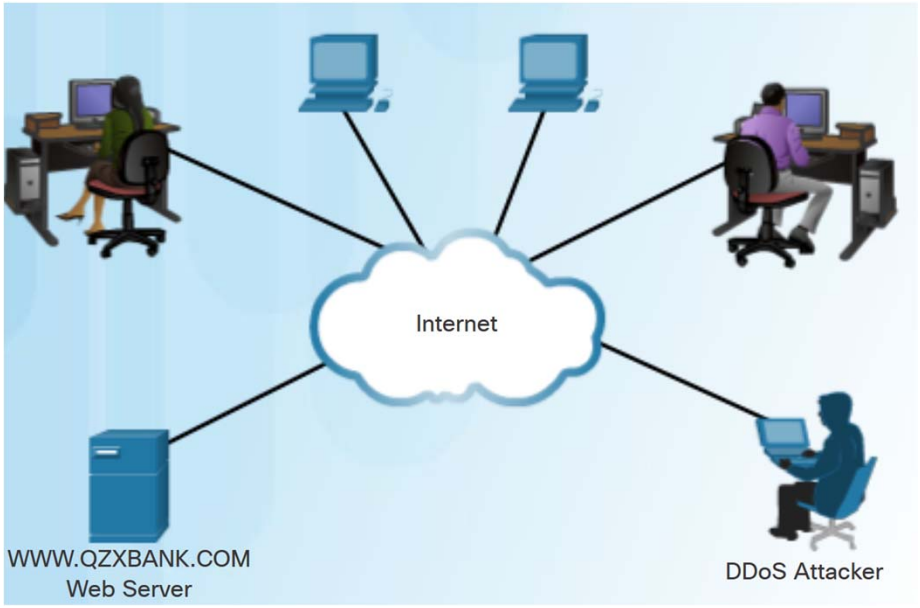


Sulmet e Rrjetit të Përbashkët
Sulmet DDoS

- Sulmet DDoS
  - Kompromenton shumë grupe
  - Burime nga burime të shumëfishta, të koordinuara
- Termat DDoS:
  - Zombies - I referohet një grupi të komprometuar (dmth., Agjentë). Këta hostë lëshojnë kodin e dëmshëm të quajtur robot (dmth. Bots).
  - Bots - Botët janë malware të dizajnuar për të infektuar një host dhe për të komunikuar me një sistem tjetër. Bots gjithashtu mund të hyn në tastet, të mbledhin fjalëkalimet, të kapin dhe të analizojnë pako, dhe më shumë.
  - Botnet - i referohet një grupi të zombies të infektuar duke përdorur malware vetë-propaguese (dmth. Bots) dhe janë të kontrolluara nga handlers.
  - Handlers - I referohet një udhëheqësi master-komandues që kontrollon grupet e zombies. Origjinatori i botnet mund të kontrollojë zombies nga distanca.
  - Botmaster - Ky është sulmuesi në kontrollin e botnet dhe handlers.



Sulmet e Rrjetit të Përbashkët
Shembull DDoS Attack

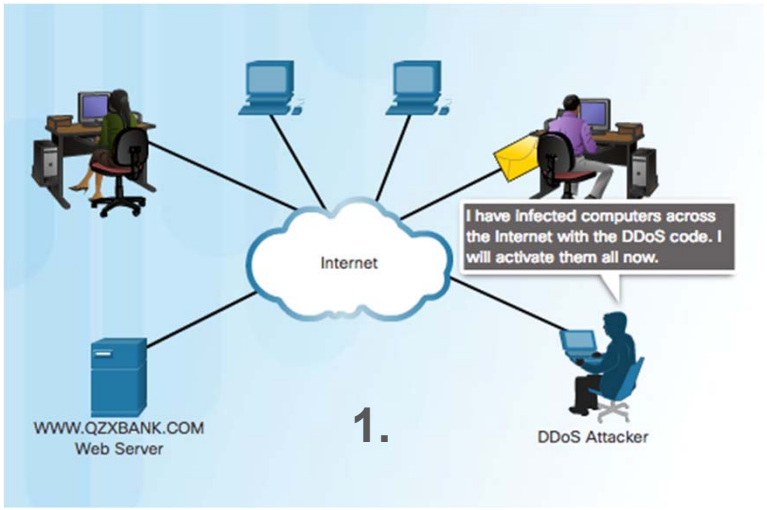


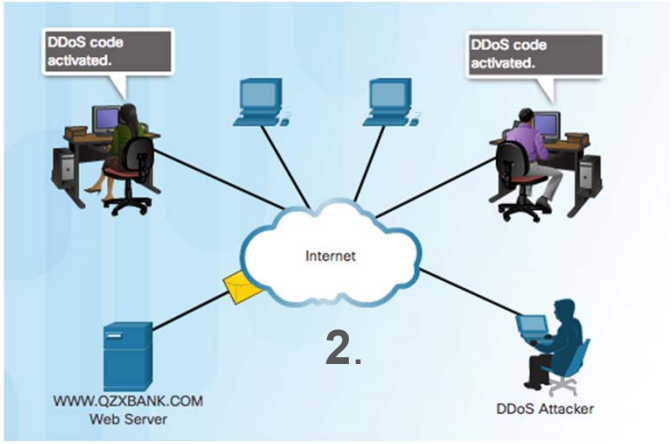
1. Sulmuesi ndërton ose blen një botnet të zombie.

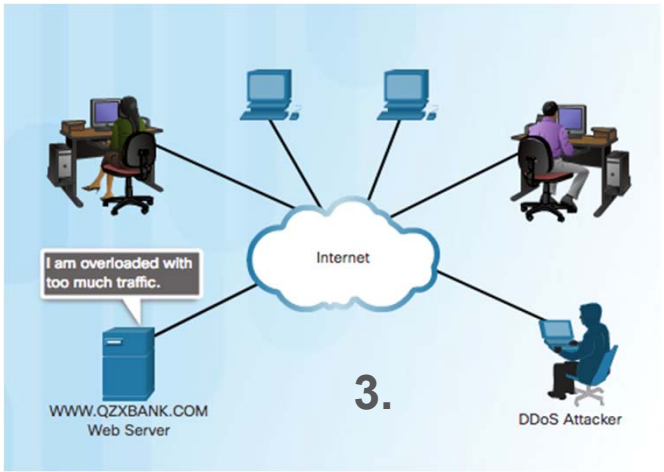
2. Kompjuterat e zombies vazhdojnë të skanojnë dhe infektojnë më shumë objektiva për të krijuar më shumë zombie.

3. Kur të jetë gati, botmaster përdor sistemet handler për të bërë botnetin e zombies të kryejnë sulmin DDoS në objektivin e zgjedhur.

Sulmet e Rrjetit të Përbashkët
Shembull DDoS Attack (Cont.)

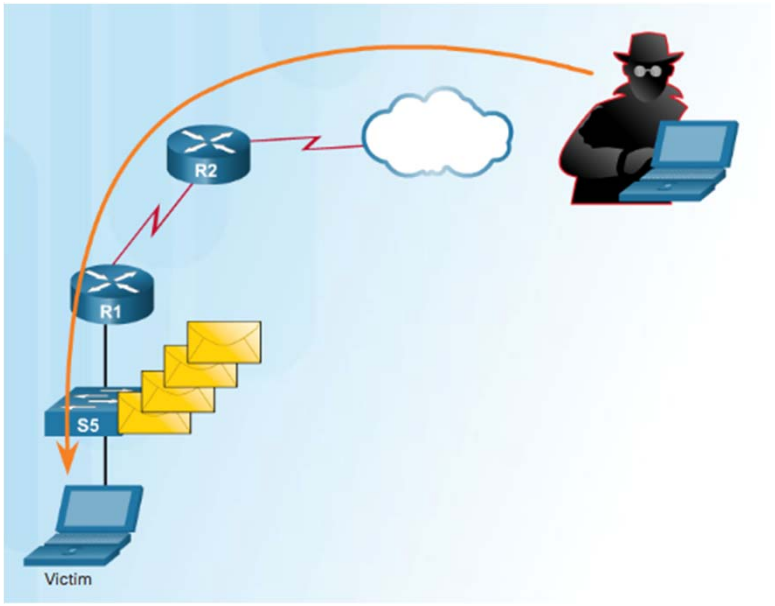






Sulmet e Rrjetit të Përbashkët
Sulmi i mbipopullimit

- Qëllimi është për të gjetur një mangësi në kujtesën e sistemit në një server dhe për ta shfrytëzuar atë.
- Shfrytëzimi i memories tampon duke e mbingarkuar atë me vlera të papritura zakonisht e bën sistemin të paoperueshëm.
- Për shembull:
  - Sulmuesi fut inputin që është më i madh se sa pritej nga aplikacioni që ekzekutohet në një server.
  - Aplikimi pranon shumën e madhe të të dhënave dhe e ruan atë në kujtesë.
  - Ai konsumon tamponin e memories të lidhur dhe potencialisht mbishkruan kujtesën ngjitur, eventualisht duke korruptuar sistemin dhe duke shkaktuar rrëzimin e saj.



Sulmet e Rrjetit të Përbashkët
Metodat e evazionit

- Sulmuesit të mësuar shumë kohë më parë se metodat malware dhe sulm janë më efektive kur ato janë të pazbuluara.
- Disa nga metodat e evazionit të përdorura nga Sulmuesit përfshijnë encryption dhe tunneling, fragmentimit të trafikut, keqinterpretimit të nivelit të protokollit, zëvendësimit të trafikut, futjes së trafikut, pivotimit dhe rootkits.
- Metodat e reja të sulmeve vazhdimisht janë duke u zhvilluar; prandaj, personeli i rrjetit të sigurisë duhet të jetë i vetëdijshëm për metodat më të fundit të sulmit në mënyrë që t'i zbulojë ato.

Përmbledhje

- Në këtë pjesë kemi trajtuar temat se si sulmohen rrjetet, llojet e kërcënimeve dhe sulmeve të përdorura nga sulmuesit.
- Sulmuesit janë hakerat gri ose të zi që përpiqen të fitojnë qasje të paautorizuar në rrjetet tona. Kriminelët kibernetikë janë sulmues të cilët janë të motivuar vetëm nga fitimi financiar.
- Sulmuesit përdorin një sërë mjetesh, duke përfshirë kriptuesit e fjalëkalimeve, Sulmin me mjetet pa tela, skanimin e rrjetit dhe mjetet e piraterisë, veglat e paketimit, paketuesit, detektorët rootkit, mjetet mjeko-ligjore, debuggers, sistemet operative për sulme, mjetet e enkriptimit, mjetet e shfrytëzimit të cenueshmërisë dhe skanerët e cenueshmërisë .
- Këto mjete mund të përdoren për përgjimin, modifikimin e të dhënave, IP spoofing, sulm në fjalëkalim, DoS, Man-in-the-middle attack, kyç i kompromet uar, network sniffing etj.

Përmbledhje

- Malware është softuer që është projektuar posaçërisht për të dëmtuar, prishur, vjedhur ose në përgjithësi të shkaktojë ndonjë veprim tjetër "të keq" ose të paligjshëm në të dhënat, hostët ose rrjetet. Tre llojet më të zakonshme të malware janë viruset, krimbat dhe kuajt e Trojës.
- Një virus është një lloj malware që propagandon duke futur një kopje të vetes në një program tjetër.
- Krimbat janë të ngjashme me viruset, sepse ata përsëriten dhe mund të shkaktojnë të njëjtin lloj dëmtimi. Ndërsa një virus kërkon një program pritës për tu aktivizuar, krimba mund të funksionojë vetë.
- Një kalë trojan është softuer që duket të jetë i ligjshëm, por përmban një kod keqdashës i cili shfrytëzon privilegjet e përdoruesit që e drejton atë.
- Sulmi më dominues aktualisht është ransomware i cili mohon qasjen në sistemin kompjuterik të infektuar ose të dhënat e tij derisa pronari paguan kriminelin kibernetik.